AP V

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**
**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

| | | |
|---|---|---|
| APPELLANTS: | Peter POST et al | CONFIRMATION NO. 5110 |
| SERIAL NO.: | 09/522,620 | GROUP ART UNIT: 2131 |
| FILED: | March 10, 2000 | EXAMINER: Shin Hon Chen |
| TITLE: | METHOD FOR PROTECTING A SECURITY MODULE AND ARRANGEMENT FOR THE IMPLEMENTATION OF THE METHOD | |



**MAIL STOP APPEAL BRIEF-PATENTS**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

**APPELLANTS' MAIN APPEAL BRIEF**

S I R:

In accordance with the provisions of 37 C.F.R. §41.37, Appellants herewith submit their main brief in support of the appeal of the above-referenced application.

**REAL PARTY IN INTEREST:**

The real party in interest is Francotyp Postalia AG and Co., a German corporation, assignee of the present application.

**RELATED APPEALS AND INTERFERENCES:**

There are no related appeals and no related interferences.

**STATUS OF CLAIMS:**

Claims 1-13 are the subject of the present appeal, and constitute all pending claims of the application. No claim was added or cancelled during prosecution.

**STATUS OF AMENDMENTS:**

No Amendment was filed in response to the final rejection.

An Amendment is being filed simultaneously herewith to correct a typographical error in claim 1. Since the Amendment is being filed simultaneously

with the Appeal Brief, the status thereof is not known at this time, however, in view of the inconsequential nature of the Amendment (correcting a typographical error), Appellants assume it will be entered, and therefore claim 1 in the Appendix attached hereto embodies this change.

**SUMMARY OF THE CLAIMED SUBJECT MATTER:**

The subject matter of the claims on appeal is a security module, of the type used in a postage meter to contain and protect security information, such as encrypted passwords, electronic funds, etc. Such a security module is plugged (potted) on a motherboard. Although the security module must be able to be replaced if and when warranted, the possibility of improper use of the security module should be assumed upon every replacement when not only is the system voltage absent, but also the replaceable battery is removed. The subject matter of the claims on appeal concerns a security module wherein such improper use can be a detected, and appropriate step then taken.

Figure 1 shows a block diagram of the security module 100 with the contact groups 101, 102 for connection to an interface 8 as well as to the battery contact posts 103 and 104 of a battery interface for a battery 134. (p. 9, l. 4-6) Although the security module 100 is potted with a hard casting compound, the battery 134 of the security module 100 is replaceably arranged on a printed circuit board outside the casting compound. (p. 9, l. 6-8) The printed circuit board carries the battery contact posts 103 and 104 for the connection of the poles of the battery 134. (p. 9, l. 8-10) The security module 100 is plugged to a corresponding interface 8 of the motherboard 9 with the contact groups 101, 102. (p. 9, l. 10-11) The first contact group 101 has a communicative connection to the system bus of a control unit, and

the second contact group 102 serves the purpose of supplying the security module 100 with the system voltage. (p. 9, l. 11-14) Address and data lines 117, 118 as well as control lines 115 proceed via the pins P3, P5-P19 of the contact group 101. (p. 9, l. 14-15) The first contact group 101 and/or the second contact group 102 is/are fashioned for static and dynamic monitoring of the plugged state of the security module 100. (p. 9, l. 15-17) The supply of the security module 100 with the system voltage of the motherboard 9 is realized via the pins P23 and P25 of the contact group 102, and a dynamic and static unplugged state detection by the security module 100 is realized via the pins P1, P2 or, respectively, P4. (p. 9, l. 17-20)

In a known way, the security module 100 has a microprocessor 120 that contains an integrated read-only memory (internal ROM; not shown) with the specific application program that the postal authority or the respective mail carrier has approved for the postage meter machine. Alternatively, a standard read-only memory ROM or FLASH memory can be connected to the module-internal data bus 126. (p. 9, l. 21 – p. 10 l. 2)

In a known way, the security module 100 has a reset circuit unit 130, an application circuit (ASIC) 150 and a logic unit 160 that serves as a control signal generator for the ASIC. The reset circuit unit 130 or the application circuit 150 and the logic unit 160 as well as further memories which may be present (not shown) are supplied with system voltage $U_{s+}$ via the lines 191 and 129, this being supplied from the motherboard when the franking device is switched on. (p. 11, l. 3-8)

Via a diode 181 and the line 136, the system voltage $U_{s+}$ is also present at the input of the voltage monitoring unit 12. A second operating voltage $U_{b+}$ is supplied at the output of the voltage monitoring unit 12, this being available via the line 138.

When the franking device is switched off, only the battery voltage $U_{b+}$ that is available, rather than the system voltage $U_{s+}$. (p. 10, l. 11-15) The battery contact post 104 at the negative pole is connected to ground. Battery voltage is supplied from the battery contact post 103 at the positive pole, to the input of the voltage monitoring unit via a line 193, via a second diode 182 and via the line 136. Alternatively to the two diodes 181, 182, a commercially available circuit can be utilized as a voltage switchover 180. (p. 10, l. 15-19)

The output of the voltage monitoring unit 12 is connected via a line 138 to an input for this second operating voltage $U_{b+}$ of the processor 120, this leading at least to a RAM memory area and guaranteeing a non-volatile storage thereat as long as the second operating voltage $U_{b+}$ is present with the required amplitude. (p. 10, l. 20-23) The processor 120 preferably contains an internal RAM 124 and a real time clock (RTC) 122 as the aforementioned RAM area. (p. 10, l. 23 – P. 11 l. 2)

The voltage monitoring unit 12 in the security module 100 executes resettable self-holding that is interrogated by the processor 120 via a line 164 and can be reset via a line 135. For resetting the self-holding, the voltage monitoring unit 12 includes a circuit, wherein the resetting is triggered only when the battery voltage has risen above the predetermined threshold. (p. 11, l. 3-7)

The lines 135 and 164 are respectively connected to terminals (pin 1 and pin 2) of the processor 120. The line 164 delivers a status signal to the processor 120, and the line 135 delivers a control signal to the voltage monitoring unit 12. (p. 11, l. 8-10)

The line 136 at the input of the voltage monitoring unit 12 also supplies the detection unit 13 with operating or battery voltage. The processor 120 interrogates

the status of the detection unit 13 via the line 139 or the detection unit 13 is triggered or reset by the processor 120 via the line 137. (p. 11, l.11-14) After being set, a static check for connection is carried out. To that end, ground potential that is present at the terminal P4 of the interface 8 of the postal security module PSM 100 is interrogated via a line 192 and can only be interrogated when the security module 100 is properly plugged in. With the security module 100 plugged in, the terminal P23 of the interface 8 is at ground potential of the negative pole 104 of the battery 134 of the postal security module PSM 100 and thus interrogation at the terminal P4 of the interface 8 can take place by the connection unit 13 via the line 192. (p. 11, l. 14-21)

A line loop that is looped back via the pins P1 and P2 of the contact group 102 of the interface 8 to the processor 120 is at the pins 6 and 7 of the processor 120. For dynamic checking of the connected state of the postal security module PSM 100 to the motherboard 9, the processor 120 applies changing signal levels to the pins 6, 7 at absolutely irregular time intervals and these are looped back via the loop. (p. 11, l. 22 – p. 12, l. 2)

The postal security module 100 is equipped with a long life battery that also enables monitoring of usage without the security module 100 being connected to the system voltage of a postal processing means. The proper use, operation, installation or integration in the suitable environment are properties to be checked by the function units of the security module 100. An initial installation is undertaken by the manufacturer of the postal security module 100. Following this initial installation, the only thing that must be checked is whether the postal security module 100 is

separated from its field of utilization (mail-processing means), this usually ensuing in the case of a replacement. (p. 11, l. 4-12)

Monitoring of this status is undertaken by the unplugged status detection unit 13. A voltage level is monitored at the pin 4 of the interface unit 8 via the connection to ground. Given replacement of the function unit, this connection to ground is interrupted, and the unplugged status detection unit 13 registers this event as stored information. (p. 12, l. 13-16) Since the storage of this information for every separation of the security module 100 from the interface unit 8 is assured by the specific, battery-operated circuit structure, an interpretation of this information can ensue at any time when a re-commissioning is desired. (p. 12, l. 17-20) The regular interpretation of this unplugged condition signal on the line 138 of the unplugged condition detection unit 13 makes it possible for the processor 120 to erase sensitive data without modifying the accounting and customer data in the NVRAM memories. (p. 12, l. 20-23) The momentary status of the postal security module with the erased, sensitive data can be interpreted as a maintenance status when replacement, repair or other similar procedures are regularly undertaken. (P. 12, l. 23 – p. 13, l. 2) Since the sensitive data of the function unit are erased, an error due to tampering with the postal security module 100 is precluded. The sensitive data are, for example, cryptographic keys. The processor 120 - in the maintenance status - prevents a core functionality of the postal security module such as, for example, an accounting and/or calculating of a security code for the security mark in a security imprint. (p. 13, l. 2-7)

To be placed back into operation, the postal security module 100 is initially plugged-in and electrically connected to the corresponding interface unit 8 of a mail

processing device. Subsequently, the device is turned on and thus the postal security module is again supplied with system voltage $U_{s+}$. Due to this specific status, the proper installation of the postal security module must now be re-checked by its function unit. To this end, a second stage of a check (dynamic plugged condition detection) is undertaken. The error-free transmission exchange of information serves as proof of the proper installation, this exchange taking place via an operative connection setup between the first function unit (processor 120) and the current loop 18 of the interface unit 8. This is a pre-requisite for a successful re-commissioning. (p. 13, l. 8-17)

A re-initialization of the sensitive data is still additionally required for status change into the normal operating condition. A communication is undertaken between the postal security module 100 and a third party, such as a remote data center, which communicates the security data. After successful communication, the unplugged condition detection unit 13 is reset, and the postal security module 100 re-assumes its normal operating condition. The re-commissioning is thus completed. (p. 13, l. 18-23)

Figure 4 shows a block circuit diagram of the postal security module PSM 100 in a preferred version. The negative pole of the battery 134 is at ground and connected to a pin P23 of the contact group 102. The positive pole of the battery 134 is connected via a line 193 to one input of the voltage switchover 180, and the line 191 carrying the system voltage is connected to the other input of the voltage switchover 180. (p. 18, l. 6-10) The output of the voltage switchover 180 is supplied to the battery monitoring unit 12 and the detection unit 13 via the line 136. The battery monitoring unit 12 and the detection unit 13 are in communication with the

pins 1, 2, 4 and 5 of the processor 120 via the lines 135, 164 and 137, 139. The output of the voltage switchover 180 also is connected via the line 136 to the supply input of a first memory SRAM that serves as a non-volatile memory NVRAM in a first technology as a result of the existing battery 134. (p. 18, l. 14-20)

The security module is in communication with the postage meter machine via the system bus 115, 117, 118. The processor 120 can enter into a communication connection with a remote data center via the system bus and a modem 83. The accounting is accomplished by the ASIC 150. The postal accounting data are stored in non-volatile memories of different technologies. (p. 18, l. 21 – p. 19, l. 2)

The system voltage is at the supply input of a second memory 114. This is a non-volatile memory (NVRAM) in a second technology (SHADOW RAM). This second technology preferably includes a RAM and an EEPROM, the latter automatically accepting the data contents given an outage of the system voltage. The NVRAM 114 in the second technology is connected to the corresponding address and data inputs of the ASIC 150 via an internal address and data bus 112, 113. (p. 19, l. 3-8)

The processor 120 of the security module 100 is connected via a module-internal data bus 126 to the memory 128 and to the ASIC 150. The memory 128 serves as a program memory and is supplied with system voltage $U_{s+}$. (p. 19, l. 19-21) The ASIC 150 of the postal security module 100 - via a module-internal address bus 110 - delivers the addresses 0 through 7 to the corresponding address inputs of the memory 128. The processor 120 of the security module 100 - via an internal address bus 111 - delivers the addresses 8 through 15 to the corresponding address inputs of the FLASH 128. The ASIC 150 of the security module 100 is in

communication with the data bus 118, with the address bus 117 and the control bus 115 of the motherboard 9 via the contact group 101 of the interface 8. (p. 19, l. 22 – p. 20, l. 6)

The processor 120 has access memories 122, 124 to which an operating voltage $U_{b+}$ is supplied from a voltage monitoring unit 12. In particular, the real time clock (RTC) 122 and the memory (RAM) 124 are supplied with an operating voltage via the line 138. The voltage monitoring unit (battery observer) 12 also supplies a status signal 164 and reacts to a control signal 135. (p. 20, l. 7-1) The voltage switchover 180 outputs the higher of its input voltages as an output voltage on the line 136 for the battery observer 12 and memory 116. Due to the capability of automatically feeding the described circuit with the higher of the two voltages $U_{s+}$ and $U_{b+}$ dependent on their amplitude, the battery 134 can be replaced during normal operation without data loss. (p. 20, l. 11-15)

In the quiescent times outside normal operation, the battery of the postage meter machine supplies the real time clock 122 with date and/or time of day registers and/or the static memory (SRAM) 124 that maintains security-relevant data in the aforementioned way. (p. 20, l. 16-19) If the voltage of the battery drops below a specific limit during battery operation, then the circuit described in the exemplary embodiment connects the feed point for the clock 122 and the static memory 24 to ground, i.e. the voltage at the clock 122 and at the static memory 124 then lies at 0 volts. (p. 20, l. 19-22) This causes the static memory 124 that, for example, contains important cryptographic keys, to be very rapidly erased. At the same time, the registers of the clock 122 are also deleted and the current time of day and the current date are lost. (p. 20, l. 22 – p. 21, l. 2) This action prevents a possible

tamperer from stopping the clock 122 of the postage meter machine by manipulation of the battery voltage without losing security-relevant data. The tamperer thus is prevented from evading security measures such as, for example, long time watchdogs.

The reset unit 130 is connected via the line 131 to the pin 3 of the processor 120 and to a pin of the ASIC 150. The processor 120 and the ASIC 150 are reset by the reset signal from the reset unit 130 when the supply voltage drops. (p. 21, l. 2-8)

Simultaneously with the indication of the under-voltage of the battery, the described circuit switches into a self-holding condition in which it remains when the voltage is subsequently increased. The next time the module 100 is switched on, the processor can interrogate the status of the circuit (status signal) and - in this way and/or via the interpretation of the contents of the erased memory - conclude that the battery voltage fell below a specific value in the interim. The processor 120 can reset the monitoring circuit, i.e. "arm" it. (p. 21, l. 9-15)

For measuring the input voltage, the unplugged status detection unit 13 has a line 192 that is connected to ground via the plug of the security module 100 and the interface 8, preferably via a socket on the motherboard 9 of the postage meter machine. (p. 21, l. 16-18) This measurement serves the purpose of statically monitoring the plugged condition and forms the basis for a monitoring on a first level. (p. 21, l. 19-20) The unplugged status detection unit 13 has a resettable self-holding capability, the self-holding being triggered when the voltage level on a test voltage line 192 deviates from a predetermined potential. (p. 21, l. 20-22) The evaluation logic includes the processor 120 connected to the other function units, the processor 120 being programmed to identify the status of the security module 100 and to

modify it. The self-holding condition can be interrogated by the processor 120 of the security module 100 via the line 139. (p. 21, l. 23 – p. 22, l. 3) The test voltage potential on the line 192 corresponds to ground potential when the security module 100 has been properly plugged. (p. 22, l. 3-6) Operating voltage potential is normally present on the line 139, ground voltage potential is present on the line 139 when the security module 100 is unplugged. The processor 120 has a fifth pin 5 to which the line 139 is connected in order to interrogate the condition of the unplugged status detection unit 13 as to whether it is connected to ground potential with self-holding. In order to reset the condition of the self-holding of the unplugged status detection unit 13 via the line 137, the processor 120 has a fourth pin 4. (p. 22, l. 7-11)

A current loop 18 is also provided that likewise connects the pins 6 and 7 of the processor 120 via the plug of the security module 100 and via the socket on the motherboard 9 of the postage meter machine. The lines at the pins 6 and 7 of the processor 120 are closed to form a current loop 18 only when the security module 100 is plugged onto the motherboard 9. This loop 18 forms the basis for a dynamic monitoring of the plugged condition of the security module 100 on a second level. (p. 22, l. 12-17)

The circuit diagram of the detection unit 13 is explained with reference to Figure 5. The unplugged status detection unit 13 includes a voltage divider that is composed of a series circuit of resistors 1310, 1312, 1314 and connected across the supply voltage, that can be tapped by a capacitor 1371, and a test voltage on the line 192. (p. 23, l. 6-9) The circuit is supplied with the system or battery voltage via the line 136. The supply voltage from the line 136 proceeds via a diode 1369 to the

capacitor 1371. An inverter is connected at the output side of the circuit and is formed by a transistor 1320 and a resistor 1398. In the normal condition, the transistor 1320 of the inverter is inhibited, and the supply voltage takes effect via the resistor 1398 on the line 139, which therefore carries logic "1", i.e. high-level in the normal condition. (p. 23, l. 10-15) A low-level on the line 139 is advantageous as the status signal for the unplugged condition because no power then flows into the pin 5 of the processor 120, thereby lengthening the life of the battery. (p. 23, l. 15-18) The diode 1369 operates together with an electrolytic capacitor 1371 to ensure that the circuit preceding the inverter is supplied with a voltage over a relatively long time span (>2s), so it still functions even though the voltage on the line 136 is absent. (p. 23, l. 18-20)

The voltage divider 1310, 1312, 1314 has a tap 1304 to which a capacitor 1306 and the non-inverting input of a comparator 1300 are connected. The inverting input of the comparator 1300 is connected to a reference voltage 1302. (p. 23, l. 21-23) The output of the comparator 1300 is connected to the line 139 via the inverter and is connected to the control input of a switch element 1322 for the aforementioned self-holding. The switch element 1322 is connected in parallel with the resistor 1310 of the voltage divider, and another switch element 1316 for resetting the self-holding is connected between the tap 1304 and ground. (p. 23, l. 23 – p. 24, l. 5) The tap 1304 of the voltage divider is at the junction of the resistors 1312 and 1314. The capacitor 1306 connected between the tap 1304 and ground prevents oscillations. The voltage at the tap 1304 of the voltage divider is compared in the comparator 1300 to the reference voltage of the source 1302. When the voltage at the tap 1304 is lower than the reference voltage of the source 1302, then

the comparator output remains switched to the low level, and the transistor 1320 of the inverter is inhibited. (p. 24, l. 5-11) As a result, the line 139 receives operating voltage potential and the status signal carries logic "1". The voltage divider is dimensioned such that, given ground potential on the line 192, the tap 1304 is at a voltage that is sure to lie below the switching threshold of the comparator 1300. (p. 24, l. 11-14) When the connection is interrupted and the line 192 is no longer connected to ground because the security module 100 was separated from the socket on the motherboard 9 or respectively, interface unit 8 of the postage meter machine, then the voltage at the tap 1304 is pulled above the voltage of the reference voltage source 1302 and the comparator 1300 switches. (p. 24, l. 14-18) The comparator output is switched to high level and, consequently, the transistor 1320 is conducting. As a result, the line 139 is connected to ground potential and the status signal carries logic "0". (p. 24, l. 18-21)

A self-hold circuit in the unplugged status detection unit 13 is realized by a transistor 1322 that is connected in parallel to the resistor 1310 of the voltage divider. The control input of this transistor 1322 is switched to high level by the comparator output. (p. 24, l. 22 – p. 25, l. 2) As a result, the transistor 1322 conducts and bridges the resistor 1310. As a result, the voltage divider is now formed only by the resistors 1312 and 1314. This causes the switchover threshold to be raised to such an extent that the comparator 1300 also remains in the switched condition when the line 192 again carries ground potential because the security module 100 was re-plugged. (p. 25, l. 2-6)

The processor 120 can reset the unplugged status detection unit 13 when a reinstallation was able to be successfully completed with the communicated data.

To that end, the transistor 1316 is made conducting by the reset signal on the line 137 and, thus, the voltage at the tap 1304 is pulled below the reference voltage of the source 1302 and the transistors 1320 and 1322 inhibit. (p. 25, l. 19-23) When the transistor 1322 is inhibited in the normal condition, then the resistors 1310 and 1312 form the upper part of the aforementioned voltage divider in series, and the switchover threshold is in turn lowered to the original level. (p. 25, l. 23 – p. 26, l. 3)

**GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL:**

The issues on appeal are as follows:

Whether the subject matter of claims 1 and 2 would have been obvious, under the provisions of 35 U.S.C. §103(a), to a person of ordinary skill in the field of security module design based on the teachings of United States Patent No. 6,105,136 (Cromer et al) in view of United States Patent No. 6,185,645 (Klein et al);

Whether the subject matter of claim 3 would have been obvious, under the provisions of 35 U.S.C. §103(a) to a person of ordinary skill in the field of security module design based on the teachings of United States Patent No. 6,059,191 (Sedlak et al) in view of Cromer;

Whether the subject matter of claims 4-8 would have been obvious, under the provisions of 35 U.S.C. §103(a) to a person of ordinary skill in the field of security module design based on the teachings of Sedlak et al and Cromer et al, further in view of United States Patent No. 4,823,323 (Higuchi);

Whether the subject matter of claim 9 would have been obvious, under the provisions of 35 U.S.C. §103(a), to a person of ordinary skill in the field of security module design based on the teachings of Sedlak and Cromer and Higuchi, further in view of United States Patent No. 5,039,580 (Mori et al);

Whether the subject matter of claims 10, 12 and 13 would have been obvious, under the provisions of 35 U.S.C. §103(a) to a person of ordinary skill in the field of security module design based on the teachings of Sedlak and Cromer et al and Mori et al; and

Whether the subject matter of claim 11 would have been obvious, under the provisions of 35 U.S.C. §103(a) to a person of ordinary skill in the field of security module design based on the teachings of Sedlak and Cromer et al and Mori et al and Higuchi.

**ARGUMENT:**

**Rejection of Claims 1 and 2 Under 35 U.S.C. §103(a) Based on Cromer et al and Klein et al**

Independent claim 1 and dependent claim 2 stand rejected under 35 U.S.C. §103(a) based on the teachings of Cromer et al and Klein et al. Appellants acknowledge that the Cromer et al reference teaches a computer system coupled to a remote computer via a data communication link, wherein the computer system includes an erasable memory element that can contain security data, such as a password. The Cromer et al reference explicitly teaches that two events can trigger erasure of the content of the erasable memory, namely a disconnection of the data communication link (column 3, lines 15-18) or activation of a tamper detection switch that detects opening of the enclosure in which the erasable memory element is located (column 3, lines 27-32).

At page 3 of the final rejection, the Examiner acknowledged that the Cromer et al reference does not explicitly disclose insertion and replacement of the security module on a motherboard, to cause resetting and re-initializing the module. The Examiner relied on the Klein reference as, according to the Examiner, disclosing

erasing the data on a module and inhibiting the functioning of a module when it is being removed form the motherboard, and re-initializing the module after insertion has taken place. The Examiner stated that it would have been obvious to a person of ordinary skill in the art to combine the teachings of Klein et al within the system of Cromer et al, because "it increases security by erasing sensitive data upon tampering and increases stability of computer system by allowing inadvertent removal of module."

First, Appellants do not agree that the Klein et al reference is concerned in any manner with erasing data from a module, whether upon removal or otherwise. The Klein et al reference is directed to avoid a computer executing a routine to be "hung up" upon removal of the wrong bus card while the routine is being executed. This is explained in the Klein et al reference at column 1, lines 58-64. The Klein et al reference is not concerned with data on the removed bus card itself, but is instead concerned with the effect that removal of the bus card, if it is the wrong bus card that is being removed, will have on the operation of the running computer system. Therefore, the Klein et al reference teaches, in one embodiment, detecting a beginning of removal of a bus card, and then removing power from the bus card and saving data from the bus card in the computer system. Although the data may be saved in the computer system, this does not necessarily mean the data are erased from the removed bus card. More importantly, if the data are security-related data, saving the data in the computer system would be self-defeating, because the purpose of erasing data in a security module is to prevent unauthorized access to the data. If the data were merely transferred to another location, as is the case in

the Klein et al reference, this would serve no purpose in protecting the data from unauthorized access.

More importantly, it is not clear how the Examiner proposes that a person of ordinary skill in the field of security module protection would precisely modify the Cromer et al reference in accordance with the teachings of Klein et al. As noted above, in the Cromer et al reference there are two possible events that could trigger erasure of data from the erasable memory. It is not clear whether the Examiner is proposing substituting the removal of a bus card for one of these erasure-triggering events, or using removal of a bus card to augment one of these erasure-triggering events. Appellants respectfully submit the references themselves provide persuasive reasons that would dissuade a person of ordinary skill in the field of security module protection from making either type of modification.

The erasure-triggering event taught in Cromer et al associated with opening of the enclosure would seem to be superfluous when applied to or combined with the teachings of Klein et al. presumably, the bus cards in Klein et al would be disposed inside of the enclosure, and therefore if erasure already occurs when the enclosure is opened, as taught by Cromer et al, there would be no need for the measures described in the Klein et al reference with regard to removal of the bus cards (module).

With regard to the other erasure-triggering event taught in Cromer et al, namely disconnection of the data link, this bears no relationship whatsoever to the reason for powering down and saving data with regard to the bus cards in the Klein et al reference, and therefore it would be a purely arbitrary substitution, without any teaching, motivation or guidance to do so in the references, to completely disregard

the teaching in Cromer et al to erase data when the communication link is disconnected, and to instead erase data when the erasable memory is removed. This would be a substantial redesign of the Cromer et al system, rather than a mere modification thereof, and is not the type of alteration that is envisioned within the scope of 35 U.S.C. §103(a).

Appellants acknowledge that in order to substantiate a rejection under 35 U.S.C. §103(a) it is not necessary for the Examiner to explicitly provide all details as to how one reference can be physically modified in accordance with the teachings of another reference. Nevertheless, Appellants submit that it is incumbent on the Examiner to propose a modification that has some hope of achieving an operable structure or system. Appellants respectfully submit that in the case of the Cromer et al and Klein et al references, the Examiner has merely proposed a combination of concepts, and this does not rise above the level of an "obvious to try" proposal, which the United States Court of Appeals for the Federal Circuit has on many occasions stated is insufficient to substantiate a rejection under 35 U.S.C. §103(a).

Claim 2 adds further steps to the non-obvious method of claim 1, and therefore is not obvious based on the teachings of Cromer et al and Klein et al for the same reasons discussed above in connection with claim 1.

**Rejection Of Claim 3 Under 35 U.S.C. §103(a) Based on Sedlak et al and Cromer et al**

Claim 3 also is directed to protecting data in a security module, and is an apparatus claim for doing so which includes a voltage monitoring unit for detecting at least one of improper use and replacement of the security module on the motherboard, and an unplugged status detection unit that inhibits functioning of the

security module during replacement thereof, and keeps the security module inhibited until the status of the unplugged status detection unit is reset.

The discussion above relating to Cromer et al applies as well to the rejection of claim 3.

As a first observation concerning the Sedlak et al reference, Appellants submit that the Sedlak et al reference, which is directed to a chip card that is insertable in a chip card reader, does not involve monitoring insertion of any components on a motherboard. All of the components shown in Figure 2 of the Sedlak et al reference are a part of an integrated circuit component, but even if this component is considered to have, or represent, a "motherboard," there is no component that is removed from, or replaced on, such a motherboard. The chip card disclosed in the Sedlak et al reference is merely inserted into contacts of a chip card reader. This is the normal, intended operation of a chip card, however, and therefore removal of the chip card from the chip card reader cannot be considered any sort of unusual event associated with the use of the chip card. This is in contrast to usage of a security module, which is intended to provide security for the overall device in which it is inserted. In the context of a security module, therefore, it is highly relevant to assume that if and when the security module is removed from its motherboard, without a proper authorization, this removal constitutes an effort at compromising the security of the device (tampering).

The circuit in the chip card disclosed in the Sedlak et al reference does include a voltage monitoring circuit, however, the details of how this voltage monitoring circuit operates are not made clear in the Sedlak et al reference. It is stated at column 6, lines 22-25, that the voltage detector circuit 20 detects when the

supply voltage (which is detected across lines GND and $V_{cc}$ in Figure 2 of Sedlak et al) exceeds or falls below the predetermined upper or lower limit values of the operating voltage, a signal is supplied to the trigger circuit 18 which, in turn, erases the contents of the RAM8. Although it is not explicitly stated in the Sedlak et al reference, the situation of no voltage being present across the lines GND and $V_{cc}$ must be within the aforementioned predetermined limits, otherwise this would result in an erasure of the contents of the RAM8 every time the chip card was removed from the chip card reader. Since such removal is an expected, normal occurrence in the usage of a chip card, removal of the chip card from the chip card reader could not possibly trigger erasure of the contents of the RAM8, since this would render the chip card useless for its intended purpose, which presumably includes multiple re-use (i.e. insertion into and removal from a chip card reader a number of times). In any event, there is no clear teaching at all in the Sedlak et al reference that it is intended or designed as a card for one-time use, which would be the case if erasure occurred every time the card was removed from the chip card reader.

Therefore, even if the chip card reader, or other components to which the chip card reader is connected, or considered by the Examiner to be the equivalent of a "motherboard," it is clear that the erasure events that are triggered in the chip card disclosed in the Sedlak et al reference cannot be triggered upon mere removal of the chip card from the chip card reader. The erasure events disclosed in the Sedlak et al reference are intended to occur while the chip card is still inserted in the reader and are intended to prevent packing of confidential information from the chip card while it is inserted in the chip card reader.

Therefore, the concept of monitoring insertion of the chip card with respect to a motherboard, as set forth in independent claims, is meaningless in the context of the chip card disclosed in Sedlak et al.

Equally as importantly, the Sedlak et al reference is completely silent as to what happens *after* erasure of the information from the RAM8 occurs. The term "reset signal" is used in the Sedlak et al reference (somewhat unconventionally) to refer to the *erasure* of information from the RAM8, rather than to restoring its contents (see, for example, column 4, lines 34-39). There is no disclosure whatsoever as to how, or even if, the contents of the RAM8 can be restored after an erasure has occurred. Lastly, again in the context of voltage monitoring, the Examiner has stated that the functioning of the card is inhibited because the RAM8 requires a voltage supply. Presumably the Examiner means that when the chip card in the Sedlak et al reference has been removed from the card reader, it is not possible to enter data into, or read data from, the RAM8. Of course, this is true, but this is trivial since the chip card is not intended to be used in any event without a chip card reader. This is another reason why monitoring a voltage indicating removal of the security module from the motherboard is meaningful in the context of a security module, but is not meaningful in the context of a chip card. Moreover, even if the chip card in Sedlak et al were removed from the card reader, there is no true "inhibition" of the RAM8, since it would operate as normal if an appropriate battery voltage were applied across the lines GND and $V_{cc}$. This is why the mere absence of voltage is not the same as "inhibiting." Claims 1 and 3 state that the inhibiting occurs by virtue of the second function unit (in claim 1) and the unplugged status detection unit (claim 2) occurs by those units being set. As long as those units

remain set, operation of the security module truly is inhibited, because even if proper voltage were restored, those units still would be set and therefore still would inhibit operation. In the subject matter of claims 1 and 3, proper operation is restored upon re-commissioning of the security module by, among other things, resetting the second function unit or the unplugged status detection unit.

Therefore, even if the Sedlak et al reference were modified in accordance with the teachings of Cromer et al, a security module as set forth in claim 3 still would not result. Equally as importantly, the above discussion demonstrates that persuasive reasons exist as to why a person of ordinary skill in the field of security module design would not even consider modifying Sedlak et al in accordance with the teachings of Cromer et al in the first place.

**Rejection Of Claims 4-8 Under 35 US.C. §103(a) Based On Sedlak et al, Cromer et al And Higuchi**

At page 5 of the final rejection, the Examiner acknowledged that Sedlak et al as modified does not explicitly disclose that the unplugged status detection unit comprises a line and a switch element for resetting the self-holding capability, the switch element being triggered by a signal from the processor on this line. The Examiner relied on the Higuchi reference as providing such a teaching. For the reasons noted above, however, the Sedlak et al reference operates in a completely different manner form the unplugged status detection unit set forth in claim 3, from which claims 4-8 depend, and therefore even if the Sedlak et al/Cromer et al combination were modified in accordance with the teachings of Higuchi, the subject matter of claims 4-8 still would not result. Claims 4-8, therefore, would not have been obvious to a person of ordinary skill in the field of security module design based on the teachings of Sedlak et al, Cromer et al and Higuchi.

**Rejection Of Claim 9 Under 35 U.S.C. §103(a) Based ON Sedlak et al, Cromer et al, Higuchi and Mori et al.**

In view of Appellants arguments above that the Sedlak et al/Cromer et al/Higuchi combination does not disclose or suggest the security module of claim 8, from which claim 9 depends, Appellants submit that even if that combination were further modified in accordance with the teachings of Mori et al, the subject matter of claim 9 still would not result. Claim 9, therefore, would not have been obvious to a person of ordinary skill in the field of security module design under the provisions of 35 U.S.C. §103(a) based on the teachings of Sedlak et al and Cromer et al and Higuchi and Mori et al.

**Rejection Of Claims 10, 12 and 13 Under 35 U.S.C. §103(a) Based On Sedlak et al, Cromer et al, and Mori et al.**

In view of Appellants arguments that the Sedlak et al/Cromer et al combination does not disclose the subject matter of claim 3, from which claims 10, 12 and 13 depend, Appellants submit that even if that combination were further modified in accordance with the teachings of Mori et al, the subject matter of claims 10, 12 and 13 still would not result. Those claims, therefore, would not have been obvious to a person of ordinary skill in the field of security module design based on the teachings of those references.

**Rejection Of Claim 11 Under 35 U.S.C. §103(a) Based On Sedlak et al, Cromer et al, Mori et al., and Higucni**

Claim 11 depends from claim 10, which in turn depends from claim 3. In view of Appellants arguments above, even if the Sedlak et al/Cromer et al/Mori et al combination were further modified in accordance with the teachings of Higuchi, the subject matter of claim 11 still would not result. Claim 11, therefore, would not have been obvious to a person of ordinary skill in the field of security module design

based on the teachings of those references under the provisions of 35 U.S.C. §103(a).

**CONCLUSION:**

For the above, Appellants respectfully submit the Examiner is in error in law and in fact in rejecting the claims on appeal. Reversal of each rejection is justified, and the same is respectfully requested.

This Appeal Brief is accompanied by a check for the requisite fee in the amount of $340.00.

Submitted by,

Steven H. Noll (Reg. 28,982)

SCHIFF, HARDIN LLP
**CUSTOMER NO. 26574**
Patent Department
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606
Telephone: 312/258-5790
Attorneys for Appellant(s).

**CERTIFICATE OF MAILING**

I hereby certify that an original and two copies of this correspondence are being deposited with the United States Postal Service as First Class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450 on November 4, 2004.

Steven H. Noll

STEVEN H. NOLL

**APPENDIX "A"**

1. A method for protecting a security module, in which security-relevant data are stored, inserted on a device motherboard, comprising the steps of:

monitoring proper insertion of said security module on said device motherboard with a first function unit, a second function unit and a third function unit in said security module;

detecting at least one of improper use and improper replacement of said security module on said motherboard with said second function unit and, upon a detection of at least one of said improper use and said improper replacement, said second function unit causing said security-relevant data to be erased;

during replacement of said security module, automatically setting said third function unit and inhibiting functioning of said security module with said third function unit as long as said third function unit is set;

following at least one of proper use and proper replacement of said security module on said motherboard, re-initializing, with said first function unit, any erased, security-relevant data; and

after said re-initializing, enabling each of said first function unit, said second function unit and said third function unit to re-commission said security module, including resetting said third function unit by said first function unit.

2. A method as claimed in claim 1 wherein the step of re-initializing comprises determining at least one of said proper use and proper replacement of said security module by establishing communication between said first function unit

and a remote data source exchanging information between said first function unit and said remote data source via current loop, and detecting that at least one of said proper use and proper replacement has occurred if said exchange of data takes place error-free.

3. A security module for insertion on a device motherboard, comprising:

a memory in which security-relevant data are stored;

a voltage monitoring unit which supplies an operating voltage to said memory to maintain said security-relevant data stored therein and which disconnects said memory from said voltage, thereby erasing said security-relevant data therein, upon occurrence of a voltage level indicating at least one of improper use and replacement of said security module on said motherboard;

an unplugged status detection unit which inhibits functioning of said security module during replacement of said security module and which has a self-holding capability, indicating that said security module has been replaced, which is triggered, for setting said unplugged status detection unit, when a voltage level on a test voltage line deviates from a predetermined voltage level; and

a processor connected to said voltage monitoring unit and to said unplugged status detection unit to re-commission said security module after at least one of said improper use and replacement on said motherboard, by enabling said voltage monitoring unit and said unplugged status detection unit, including resetting said unplugged status detection unit.

4. A security module as claimed in claim 3 wherein said unplugged status detection unit comprises a line and switch element for resetting said self-holding capability, said switch element being triggered by a signal from said processor on said line.

5. A security module as claimed in claim 4 wherein said unplugged status detection unit comprises:

a voltage divider comprising a series resistor circuit connected across a terminal for receiving a supply voltage, tapped by a capacitor, and a line having a test voltage thereon;

a diode connected between said terminal for receiving a supply voltage and said capacitor;

a comparator having a non-inverting input, an inverting input connected to a reference voltage source, and a comparator output;

a further capacitor tapping said voltage divider and connected to said non-inverting input of said comparator;

said comparator output being connected to a line at a voltage potential via an inverter;

a switch element having a control input connected to said comparator output, said switch element producing said self-holding capability and being connected in parallel with a resistor of said voltage divider; and

said switch element for resetting said self-holding capability being connected between said voltage divider tap for said further capacitor, and ground.

6. A security module as claimed in claim 5 further comprising an interrogation line connected between said processor and said unplugged status

detection unit for interrogating a self-holding status of said unplugged status detection unit by said processor.

7. A security module as claimed in claim 6 wherein said line having said test voltage thereon is at ground potential, and wherein said line at a voltage potential connected to said comparator output is at operating voltage potential when said security module is plugged into said device motherboard and is otherwise at ground potential when said security module is not plugged into said device motherboard.

8. A security module as claimed in claim 3 wherein said memory is contained in said processor and is at an operating voltage supplied from said voltage monitoring unit as long as said processor is supplied with system voltage, and wherein said processor has a terminal for resetting said self-holding capability of said unplugged status detection unit, and a further terminal for interrogating a status of said unplugged status detection unit.

9. A security module as claimed in claim 8 further comprising an ASIC connected to said processor via an internal data bus, said ASIC having a first contact group for connection to a system bus of a device containing said device motherboard.

10. A security module as claimed in claim 3 further comprising a printed circuit board on which said processor, said voltage monitoring circuit and said unplugged status detection unit are mechanically and electrically mounted, said printed circuit board having contact terminals for a battery;

a security module housing formed by a hard casting compound surrounding said printed circuit board and said processor, said voltage monitoring

circuit and said unplugged status detection circuit thereon, with said contact terminals being exposed to an exterior of said housing;

a battery replaceably connected to said contact terminals outside of said housing; and

said printed circuit board having a first contact group, accessible from outside of said housing, for communicating with a system bus of a device containing said device motherboard, and a second contact group accessible from an exterior of said housing for receiving system voltage, and at least one of said first contact group and said second contact group being connected to said unplugged status detection unit to monitor a plugged status of said security module.

11. A security module as claimed in claim 10 wherein said processor includes terminals for monitoring said plugged status of said security module with lines forming a current loop when said security module is plugged into said device motherboard.

12. A security module as claimed in claim 3 wherein said processor has a terminal for emitting at least one signal identifying a status of said security module.

13. A security module as claimed in claim 12 wherein said processor is connected to an input/output unit having input/output ports, and having at least one internal signaling element in said security module connected to said input/output ports.